

AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions, and listings, of claims in the application:

1-43. (Cancelled)

44. (currently amended) A tamper-resistant security device for use in a user device comprising:

memory for storing user credentials, including at least a security key associated with a user of the user device;

an Authentication and Key Agreement (AKA) module for performing an AKA process with said security key;

a hardware communications interface for receiving one or more external AKA process commands from a device external to the tamper-resistant security device and returning processing results performed in the tamper-resistant security device in response to the one or more AKA process commands;

a cooperating application, contained within the tamper-resistant security device and having been given access rights to access the AKA module, configured to selectively receive the one or more AKA process commands and selectively provide enhanced security processing of the one or more AKA process commands; and

an application interface internal to the tamper-resistant security device for interfacing said AKA module and said cooperating application so that the cooperating application performs the enhanced security processing in conjunction with the AKA module within the tamper-resistant security device,

wherein said enhanced security processing by said cooperating application includes post-processing of at least one AKA output parameter produced by the AKA module in response to the one or more AKA process commands, said post-processing including encapsulation of said at least one AKA output parameter to generate a further AKA parameter that has higher security than said at least one AKA output parameter produced in response to the one or more AKA process commands.

45. Canceled.

46. (currently amended) The tamper-resistant security device according to claim 44, wherein said enhanced security processing includes ~~at least one of:~~

- pre-processing of at least one AKA input parameter, ~~and~~
- ~~post processing of at least one AKA output parameter.~~

47-48. Canceled.

49. (previously presented) The tamper-resistant security device according to claim 44, wherein said enhanced security processing includes evaluation of a predetermined number of consecutive AKA input parameters for verifying that said AKA input parameters can be used securely.

50. (previously presented) The tamper-resistant security device according to claim 49, wherein said enhanced security processing further includes combination of a predetermined

number of consecutive AKA output parameters generated in response to a number of corresponding unique AKA input parameters.

51. (previously presented) The tamper-resistant security device according to claim 44, further comprising;

means for registration or detection of information representative of security conditions in relation to said tamper-resistant security device; and

means for performing security policy processing based on said information.

52. (previously presented) The tamper-resistant security device according to claim 51, wherein the security conditions reflect at least one of an environment in which said security device is operated and a network interface over which a request for AKA processing originates.

53. (previously presented) The tamper-resistant security device according to claim 51, wherein said security policy processing includes at least one of a security policy decision process and a security policy enforcement process.

54. (previously presented) The tamper-resistant security device according to claim 51, wherein said means for performing security policy processing comprises means for selectively disabling direct access to said AKA module.

55. (previously presented) The tamper-resistant security device according to claim 51, wherein said tamper-resistant security device comprises means for detecting whether said

tamper-resistant security device is operated in its normal environment or in an environment considered insecure, and said means for performing security policy processing comprises means for disabling direct access to said AKA module when operated in said insecure environment.

56. (previously presented) The tamper-resistant security device according to claim 44, wherein said cooperating application includes a security enhancing application, and said security device further comprises means for transferring a request for AKA processing directly to said AKA module if said security device is operated in an environment considered secure, and means for transferring said request to said security enhancing application if said security device is operated in an environment considered insecure.

57. (previously presented) The tamper-resistant security device according to claim 44, wherein said cooperating application is performing at least part of the computations in connection with end-to-end key agreement between users.

58. (previously presented) The tamper-resistant security device according to claim 44, wherein said cooperating application is masking key information generated by said AKA module.

59. (previously presented) The tamper-resistant security device according to claim 44, wherein said cooperating application is a software application installed in an application environment of said tamper-resistant security device.

60. (currently amended) The tamper-resistant security device according to claim 59, wherein said cooperating application is securely downloaded into said tamper-resistant security device from a trusted party.

61. (previously presented) The tamper-resistant security device according to claim 44, wherein said cooperating application is a privacy enhancing application, which participates in managing a user pseudonym.

62. (previously presented) The tamper-resistant security device according to claim 61, wherein said privacy enhancing application is ~~requesting~~ configured to request an AKA response from said AKA module based on an old user pseudonym and ~~for generating~~ generate a previously presented user pseudonym based on the received AKA response.

63. (withdrawn) The tamper-resistant security device according to claim 44, wherein the application is a software application implemented in an application environment of said tamper-resistant security device and adapted for cooperating with said AKA module, and said AKA module is also implemented, at least partly, as a software application in said application environment.

64. (withdrawn) A user terminal provided with a tamper-resistant security device according to claim 44.

65. (withdrawn) The user terminal according to claim 64, wherein said cooperating application is at least one of a security enhancing application and a privacy enhancing application.

66. (withdrawn) The user terminal according to claim 64, wherein said cooperating application is performing enhanced security processing of at least one parameter associated with said AKA process.

67. (withdrawn) The user terminal according to claim 66, wherein said enhanced security processing includes encapsulation of said at least one AKA parameter for producing an output parameter of higher security than said at least one AKA parameter.

68. (withdrawn) The user terminal according to claim 64, further comprising means for performing security policy processing based on information representative of security conditions in relation to said tamper-resistant security device.

69. (withdrawn) The user terminal according to claim 68, wherein the security conditions reflect at least one of the environment in which said security device is operated, the network interface over which a request for AKA processing comes, and the network used by the user terminal for network communication.

70. (withdrawn) The user terminal according to claim 68, wherein said security policy processing includes at least one of a security policy decision process and a security policy enforcement process.

71. (withdrawn) The user terminal according to claim 68, wherein said means for performing security policy processing is implemented in said tamper-resistant security device for selectively disabling direct access to said AKA module.

72. (withdrawn) The user terminal according to claim 64, wherein said cooperating application is a security enhancing application, and said security device further comprises means for transferring a request for AKA processing directly to said AKA module if said security device is operated in an environment considered secure, and means for transferring said request to said security enhancing application if said security device is operated in an environment considered insecure.

73. (withdrawn) The user terminal according to claim 64, wherein said cooperating application includes a security enhancing application, and said user terminal further comprises means for transferring a request for AKA processing directly to said AKA module if said request comes over an interface considered secure, and means for transferring said request to said security enhancing application if said request comes over an interface considered insecure.

74. (withdrawn) The user terminal according to claim 73, wherein said security enhancing application comprises a number of different security enhancing modules, and said

security enhancing application is for selecting among said security enhancing modules in dependence on the type of interface.

75. (withdrawn) The user terminal according to claim 64, wherein said cooperating application is a software application installed in an application environment of said tamper-resistant security device.

76. (withdrawn) The user terminal according to claim 64, wherein said cooperating application includes a security enhancing application authenticating a network over which said user terminal intends to communicate.

77. (withdrawn) A network server managed by a trusted party sharing a security key with a tamper-resistant security device implemented in a user terminal according to claim 64.

78. (withdrawn) The network server according to claim 77, wherein said download application is at least one of a security enhancing application, a privacy enhancing application, and a security policy application.

79. (new) The tamper-resistant security device according to claim 44, wherein said one or more AKA process commands include a random challenge and said at least one AKA output parameter includes a response to the random challenge that matches the random challenge.

80. (new) The tamper-resistant security device according to claim 79, wherein said response is encapsulated using a function applied to manipulate the response to produce a higher security response.

81. (new) The tamper-resistant security device according to claim 80, wherein said function is a keyed function.

82. (new) The tamper-resistant security device according to claim 81, wherein said said one or more AKA process commands include multiple random challenges and said at least one AKA output parameter includes multiple responses to the random challenges and said function is a keyed function of the multiple responses.